(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 09269916 A

(43) Date of publication of application: 14.10.97

(51) Int Cl G06F 12/14
G06F 17/21
G09C 1/00
G09C 1/00

(21) Application number: 09015010

(22) Date of filing: 29.01.97

(30) Priority: 02.02.96 JP 08 17338

(71) Applicant: HITACHI LTD

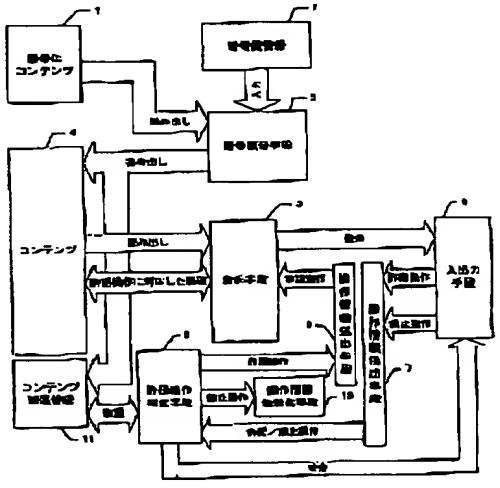
(72) Inventor: NAKADA JUNJI
YANAGI KUNIHIRO
KINUKAWA HIROYUKI
MIZUNO TSUTOMU

# (54) ELECTRONIC INFORMATION DISTRIBUTION METHOD

(57) Abstract

PROBLEM TO BE SOLVED: To provide a means for preventing the distribution of a content secondary product without a notice by means of the rightful user of content without restricting content types and a display means.

SOLUTION: A ciphered content 1 and a cipher key information 2 are inputted to a cipher decoding means 3, and the content 4 and content related information 11 are written. The content 4 is displayed by the display means 5 corresponding to the content type and it is used by the use using an input/output means 6. Operation information which is transmitted from the input/output means 6 to a display means 5 is once taken out by an operation information extraction means 7 and a permission operation judgment means 8 judges whether the pertinent operation is a permitted operation or an inhibited operation. For judgment, content related information 1 is referred to. When the permission operation judgment means 8 judges the permission operation, pertinent operation information is transmitted to the display means 5 by using an operation information transmission means 9. When it judges the inhibition operation, pertinent operation information is invalidated by an operation, information invalidating means 10.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－269916

(43)公開日　平成９年(1997)10月14日

| (51)Int.Cl.[6] | | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|---|
| Ｇ０６Ｆ | 12/14 | ３２０ | | Ｇ０６Ｆ | 12/14 | ３２０Ａ |
| | | | | | | ３２０Ｂ |
| | 17/21 | | 7259－5Ｊ | Ｇ０９Ｃ | 1/00 | ６４０Ｚ |
| Ｇ０９Ｃ | 1/00 | ６４０ | 7259－5Ｊ | | | ６６０Ｄ |
| | | ６６０ | 7259－5Ｊ | | | ６６０Ｅ |

審査請求　未請求　請求項の数８　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－15010

(22)出願日　平成９年(1997)１月29日

(31)優先権主張番号　特願平8－17338

(32)優先日　平８(1996)２月２日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　中田　順二
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　柳　邦宏
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　絹川　博之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

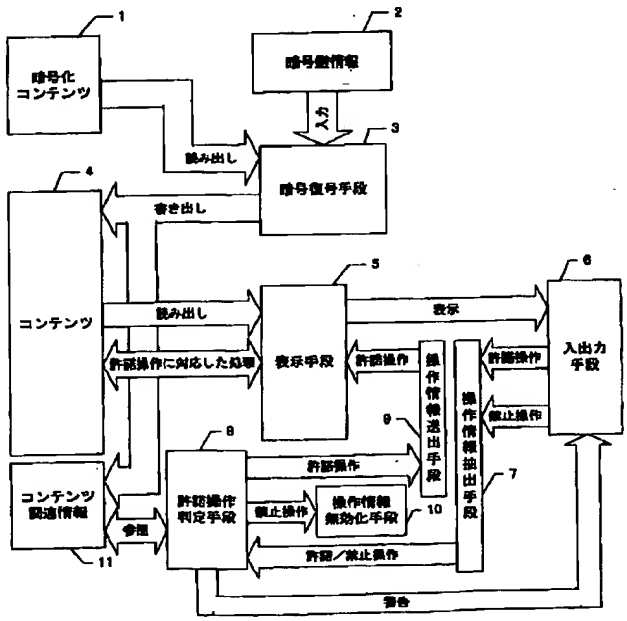
(54)【発明の名称】　電子情報配布方法

(57)【要約】

【課題】コンテンツタイプや表示手段を限定することなく、コンテンツの正当な利用者によるコンテンツ二次生成物の無断配布を防止する手段を提供する。

【解決手段】暗号化コンテンツ１と暗号鍵情報２が暗号復号手段３に入力され、コンテンツ４とコンテンツ関連情報１１が書き出される。コンテンツ４はコンテンツタイプに対応した表示手段５により表示され、入出力手段６を用いる利用者により利用される。入出力手段から表示手段へ送られる操作情報は、一旦操作情報抽出手段７によって取り出され、許諾操作判定手段８によって、当該操作が許諾された操作に当たるか禁止された操作にあたるかが判定される。判定にあたっては、コンテンツ関連情報１１も参考にする。許諾操作判定手段８によって許諾操作にあたると判定された場合は、当該操作情報を操作情報送出手段９を用いて表示手段５へ送出し、禁止操作にあたると判定された場合は、当該操作情報を操作情報無効化手段１０によって無効化する。

図1



1

【特許請求の範囲】

【請求項１】暗号化されたコンテンツを受信する受信手段と、前記暗号化されたコンテンツを復号するために必要な暗号鍵情報を記憶する記憶手段と、前記暗号化鍵を用いて暗号化されたコンテンツを復号する手段と、復号されたコンテンツを表示するための手段とを備えた表示装置へ前記暗号化されたコンテンツ配布する電子情報配布方法において、

前記表示装置の操作者が入力した操作情報が許諾された操作にあたるか禁止された操作にあたるかを判定し、

許諾された操作にあたると判定された場合は、前記暗号鍵を用いて前記表示装置が受信した暗号化されたコンテンツを復号して、前記表示装置に前記暗号化されたコンテンツに関連し前記操作情報に対応する表示を行い、

禁止された操作にあたると判定された場合は、前記暗号化されたコンテンツに関連する表示を禁止することを特徴とする電子情報配布方法。

【請求項２】請求項１に記載の電子情報配布方法において、

前記表示手段は、前記暗号化されたコンテンツと共に、前記暗号化されたコンテンツに関連した情報を受信し、

前記操作情報が許諾された操作にあたるか禁止された操作にあたるかの判定は、前記コンテンツに関連する情報を用いて行うことを特徴とする電子情報配布方法。

【請求項３】請求項１または２に記載の電子情報配布方法において、

前記操作情報が禁止された操作にあたると判定された場合は、警告を発することを特徴とする電子情報配布方法。

【請求項４】請求項３に記載の電子情報配布方法において、

前記警告を発すると共に、前記コンテンツに関連する情報を表示することを特徴とする電子情報配布方法。

【請求項５】請求項１または２に記載の電子情報配布方法において、

前記操作情報が禁止された操作にあたると判定された場合は、前記表示装置の表示を終了することを特徴とする電子情報配布方法。

【請求項６】請求項２乃至５のいずれかに記載の電子情報配布方法において、

前記暗号復号手段は、前記暗号化されたコンテンツを揮発性記憶上に書き出し、前記コンテンツに関連する情報を不揮発性記憶上に書き出すことにより前記暗号化されたコンテンツを復号することを特徴とする電子情報配布方法。

【請求項７】請求項２乃至６のいずれかに記載の電子情報配布方法において、

前記コンテンツに関連する情報として、前記暗号化されたコンテンツの著作権情報、前記暗号化されたコンテンツの配布対象となった利用者情報および前記暗号化されたコンテンツの配布を行った配布者情報のうち少なくとも１つを含むことを特徴とする電子情報配布方法。

2

【請求項８】暗号化されたコンテンツを受信する受信手段と、前記暗号化されたコンテンツを復号するために必要な暗号鍵情報を記憶する記憶手段と、前記暗号化鍵を用いて暗号化されたコンテンツを復号する手段と、復号されたコンテンツを表示するための手段とを備えた表示装置において、

前記表示装置の操作者が入力した操作情報が許諾された操作にあたるか禁止された操作にあたるかを判定する手段を有し、

前記表示するための手段は、許諾された操作にあたると判定された場合は、前記暗号鍵を用いて前記表示装置が受信した暗号化されたコンテンツを復号して、前記表示装置に前記暗号化されたコンテンツに関連し前記操作情報に対応する表示を行い、禁止された操作にあたると判定された場合は、前記暗号化されたコンテンツに関連する表示を禁止することを特徴とする表示装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、不特定多数の者に対して電子化された情報（コンテンツ）を配布可能なネットワークに係るものである。その中でも特に、配布されるコンテンツにおける著作権者の著作権を保護する電子情報配布方法および電子化された情報に関連するものを表示する表示装置に関する。

【０００２】

【従来の技術】電子的な著作物は常に複製の危機にさらされている。代表的なものがコンピュータソフトウェアである。最近では、違法コピーを通報すると賞金を与える団体まで現れるほどの切実な問題である。コンピュータソフトウェアは、配布したフロッピーディスクが破損した場合などに備えて、私的用途に限ってバックアップのための複製を作成することが一般に認められている。このため、配布されているフロッピーディスク自体にはそれほど厳しいコピープロテクト手段が施されてはいない。

【０００３】そこで、一般に、著作権保護に関しては、配布したコンピュータソフトウェアの起動時に著作権者の表示を行うことにより利用者に注意を促す、という手段をとっている。また、ソフトウェアのインストール時にユーザーの氏名や所属を入力させることにより、ソフトウェアの起動毎に誰に対してライセンスされたものかを表示するようにしているものも多い。

【０００４】一部に、パラレルポート等に接続するハードウェアを利用したコピープロテクト手段を取るソフトウェアベンダーもあるが、ソフトウェアのコスト高につながるためあまり普及していない。

【０００５】ところで、ここまで述べたコンピュータソフトウェアの一般的な著作権保護方式はプログラムが中

心で、プログラムを用いて作成したデータ（以下コンテンツと記す）の保護については考慮されていない。インターネット時代では、コンテンツの複製防止も重要な課題である。

【０００６】コンテンツの複製防止や著作権表示に関しては、特開平４－２３３０４３号公報「データ処理方法及びデータ処理装置」（従来例１）にその一例が見られる。これは、ＳＧＭＬ（Standard Generalized Markup Language）文書のタグを拡張して「著作権情報」や「複写禁止属性」を文書に持たせることで、ディスプレイへの表示やプリンタでの印刷において著作権表示を行なったり、文書の複写や送信のコマンドを無効にする機能を付加したものである。

【０００７】一方、複製した文書の漏洩先を発見するという観点からは、特開平２－９７１４６号公報「文書管理装置」（従来例２）にその一例が見られる。これは、文書を平文の形態で全体の意味を保存したまま、配送先対応に一部分だけを変換し、漏洩した文書から配送先を特定するものである。具体的には、配送先対応に文書中の文字間隔や行間隔を微妙に変更し、変更前の原文書との差分を取ることで実現している。

【０００８】ところで、ソフトウェアまたはコンテンツの不正な複製防止に暗号を用いる方式も実用化されている。信学技法ＩＳＥＣ９４－１８「ＣＤ－ＲＯＭによるソフトウェア流通技術」（従来例３）にその一例が見られる。暗号化したソフトウェアまたはコンテンツをＣＤ－ＲＯＭで事前に配布し、復号鍵を有償で事後に配布することにより、ソフトウェアまたはコンテンツの不正な複製利用の防止を狙っている。

【０００９】

【発明が解決しようとする課題】しかし、従来例１では、コンテンツタイプがＳＧＭＬ文書に限られ、また、発明を実現する上で、独自に拡張したＳＧＭＬ文書タグを解釈して実行する専用装置もしくは専用ソフトウェアが必要になる。また、一般的なテキストエディタで装置に格納されたＳＧＭＬ文書を読み出すことが可能ならば、容易に「著作権情報」や「複写禁止属性」のタグを除去することができるため、ＳＧＭＬ文書の読み出し手段は前記専用装置もしくは専用ソフトウェアに限られなければならない。以上のように、コンテンツの形式や表示手段が限定的であるのは、コンテンツの広範囲な流通を図る上での妨げとなる。これに対して、多様なコンテンツタイプや表示手段に対応可能な複製防止手段を提供するのが本発明の第１の課題である。

【００１０】一方、従来例２においても、コンテンツタイプが英文テキストなどの特定のイメージ情報に限られてしまうという問題があるが、表示手段はイメージ情報が表示可能であれば何でもよく、印刷物に形を変えても有効であるという点が従来例１と異なる。しかし、この発明では漏洩したコンテンツから漏洩元を特定するため



には、同コンテンツが配送先対応の差分情報を保管している端末へ回収されなければならない。このため、コンテンツの不正な漏洩が速やかに検出できるわけではなく、また、漏洩したコンテンツを手にした誰でもがコンテンツから漏洩元を特定できるわけではない。これに対して、漏洩したコンテンツからコンテンツが漏洩したことの判別とコンテンツ漏洩元の特定が誰でもできるようにすれば、不正な複製配布防止には有効と考えられる。これが、本発明の第２の課題である。

【００１１】従来例３は、暗号を使ってソフトウェアの不正な複製利用の防止を狙った実例である。確かに、暗号化したコンテンツを格納したＣＤ－ＲＯＭの保有者がコンテンツを利用するためには復号鍵を入手する必要があり、復号鍵を有償で配布することを前提にしておけば、暗号を使ったコンテンツ販売が可能になる。しかし、復号鍵を正当に入手した利用者が、復号したコンテンツを複製配布するのを防ぐための手段は提供されておらず、著作権保護の観点からはまだ課題が残されていると言える。

【００１２】従来例３に代表されるような、暗号を使ったコンテンツ配布における一般的な課題を図２に示す。図２において、暗号化コンテンツ１は何らかの手段で暗号鍵情報２とともに利用者の端末上で暗号復号手段３に入力され、コンテンツ４が端末上のいずれかの記憶装置に書き出される。コンテンツ４のコンテンツタイプは従来例１で述べたＳＧＭＬ文書に限らず、イメージ情報や音声情報などあらゆるタイプが考えられるが、各々のタイプに対応した表示手段５があらかじめ端末上に存在するものとする。

【００１３】コンテンツ４は表示手段５を介して入出力手段６により利用されるが、コンテンツ利用における操作方法としては、大きく分けて、法的もしくは利用契約上許諾されている操作（閲覧など）と禁止されている操作（送信、編集など）がある。従来例１では、ある特殊な表示手段を前提として禁止操作を無効にしていたが、多様なコンテンツタイプに対応するためには表示手段５を限定することは困難である。すなわち、一般には図に示したように、禁止操作に対応した処理が実行されて、コンテンツの二次生成物１２が端末上に作成される。このような二次生成物の作成を防止するのが本発明の第３の課題である。

【００１４】

【課題を解決するための手段】以上の課題を解決するために、本発明では、図１に示すように、入出力手段６から表示手段５に加えられる操作情報を抽出する手段７と、抽出した操作情報が許諾された操作にあたるか禁止された操作にあたるかを判定する手段８と、許諾された操作にあたると判定された場合は当該操作情報を表示手段５に送出する手段９と、禁止された操作にあたると判定された場合は当該操作情報を無効化する手段１０とを

設けた。また、禁止された操作と判定された場合は、許諾操作判定手段９が入出力手段６に対して警告を発する手段も設けた。

【００１５】そして、暗号化コンテンツ１はコンテンツ４の他にコンテンツ関連情報１１を含み、暗号復号手段３によってそれぞれ端末上に書き出される。コンテンツ関連情報１１はコンテンツ４に関連する一般的な情報を提供する目的と、許諾操作に関する情報を提供する目的とを担っている。

【００１６】以上の内容は、表示手段５やコンテンツ４のコンテンツタイプを特定することなく実現可能であり、コンテンツ４そのものに対する禁止操作（送信、編集など）を防止しつつ、コンテンツ関連情報１１は随時参照可能な構成となっている。

【００１７】

【発明の実施の形態】次に図３～図９を用いて、本発明を、インターネットを利用したコンテンツ配布に適用した一実施例について説明する。図３はシステム図、図４はデータ処理フロー、図５はコンテンツの利用方法の概要、図６～図８は利用方法の詳細、図９は表示手段とメッセージー操作対応表の例である。

【００１８】図３において、コンテンツ４に関する著作（権）者や作成年月日などの著作権情報１１１が著作権管理部１１４を用いて、また、利用者に関する利用者情報１１２が利用者管理部１１５を用いて予め登録してあるものとする。以下、図５の各ステップ（Ｓｎ）に沿って説明する。

【００１９】（Ｓ１）：まず、利用者はブラウザ２０を用いてインターネット１８経由でサーバ１３にアクセスし、情報発信・アクセス制御部１７を介して、コンテンツ紹介情報１４を参照する。コンテンツ紹介情報１４は見出し風のものでも良いし、何らかのコンテンツ検索機能を持っていてもよい。とにかく、所望のコンテンツ４を特定できるための情報が提供されるものとする。

【００２０】（Ｓ２）：次に、利用者はサーバ１３に対して所望のコンテンツ４を要求する。要求内容は（Ｓ１）と同様の経路でサーバに送られ、ブラウザ要求処理部１５に渡される。

【００２１】（Ｓ３）：ブラウザ要求処理部１５が要求に応じた処理を行う。具体的には、図６に示すように、コンテンツ４を要求してきた利用者情報１１２を検索して認証処理を行い（Ｓ３１）、要求されたコンテンツ４を検索し（Ｓ３２）、コンテンツの著作権情報１１１を検索し（Ｓ３３）、誰が何を誰にいつ配布したかを記録する配布情報１１３を生成して配布管理部１１６で管理し（Ｓ３４）、コンテンツ４とコンテンツ関連情報１１１（著作権情報１１１と利用者情報１１２と配布情報１１３）を結合し（Ｓ３５）、暗号処理部１６で暗号化して（Ｓ３６）、暗号化コンテンツ１として送信する（Ｓ３７）。



【００２２】（Ｓ４）：端末１９はサーバから送られてきた暗号化コンテンツ１を受信して、復号ソフト２１で処理する。

【００２３】（Ｓ５）：復号ソフト２１での処理内容を図４と図７を用いて説明する。暗号化コンテンツ４と暗号鍵情報２を暗号復号手段３に入力して復号する（Ｓ５１）。この場合、暗号鍵情報２の入手タイミングは、事前に配布されていてもよいし、事後に配布されていてもよいし、暗号化コンテンツ４と同時でもよい。続いて、暗号復号手段３はコンテンツ４を揮発性記憶２３上に書き出し（Ｓ５２）、コンテンツ関連情報１１を不揮発性記憶２４上に書き出す（Ｓ５３）。続いて、暗号復号手段３は表示手段５を呼び出して（Ｓ５４）、復号したコンテンツ４の読み出しを指示する（Ｓ５５）。

【００２４】（Ｓ６）：表示手段５がコンテンツ４を表示する。

【００２５】（Ｓ７）：表示手段５によってコンテンツ４が表示されたら操作監視モードに入る。操作監視モードの実現方法を図４と図８を用いて説明する。まず、ユーザー操作が貯えられるメッセージキュー２７から表示手段５に送られる全てのメッセージをフック２６を用いて抽出する。ここで、メッセージ、メッセージキュー、フックについて簡単に説明する。

【００２６】複数のウィンドウを開いて、複数のプロセスを同時に実行させることが可能なオペレーティングシステム（以下ＯＳと記す）では、通常、ユーザープロセス間やプロセスープロセス間の通信に、あるフォーマットに従ったメッセージを用いている。これらのメッセージを貯めて逐次適当なプロセスに送り出すものがメッセージキューであり、やりとりされているメッセージを取り出す仕組みがフックで、通常はＯＳの機能として備わっている。

【００２７】フック２６を用いて抽出したメッセージは、表示手段毎の「メッセージー操作対応表」を参照してどのような操作にあたるかを調べ（Ｓ７２）、複製・編集判定手段２５が複製・編集操作にあたると判定した場合は（Ｓ７３）、警告を表示し（Ｓ７４）、表示手段５に対して終了命令を発行する（Ｓ７５）。複製・編集操作にあたらない場合は引き続いてフック７１による操作の監視を継続する（Ｓ７６）。

【００２８】図９に「メッセージー操作対応表」の例を示す。図９において、表示手段画面の一例９０１は、図のようなメニュー構造を持つものとする。各メニューをユーザーが操作する時に発生するメッセージにはメニューに対応したパラメータ（例えば“上書き保存”であれば&１０３Ｈ）が含まれているため、メッセージをフックして調べることにより、当該操作がどのような操作にあたるのかを判別することができる。このような、メッセージー操作対応表９０２を表示手段名９０３ごとに保持しておくことで、多様な表示手段５に対応した操作監

視が実現できる。

【００２９】以上、本実施例では特にコンテンツ関連情報１１について言及していないが、これは、復号ソフト２１による暗号化コンテンツ１の復号に先立って画面に表示されても良いし、複製・編集判定手段２５から発行される警告に付随して表示されてもよい。また、任意のタイミングで利用者が参照してもよい。

【００３０】また、本実施例では、複製／編集操作にあたると判定されるとすかさず表示手段５を終了するようにしているが、警告を発行するだけでもかまわない。

【００３１】また、本実施例では、禁止操作としてあらかじめコンテンツの複製と編集操作だけを前提としているが、禁止操作に関する情報をコンテンツ関連情報１１に持たせ、これを参照することにより、禁止操作にあたるかどうかを判定してもよい。

【００３２】また、本実施例では、復号したコンテンツ４を揮発性記憶２３上に、コンテンツ関連情報１１を不揮発性記憶上に書き出している。これは、システムの不意な異常終了に際しても、コンテンツ４が復号されたままで端末１９上に残らないようにするためであるが、端末資源の関係上、揮発性記憶の確保が容易でない場合などには、コンテンツ４を不揮発性記憶上に復号することも可能である。

【００３３】

【発明の効果】本発明によると、利用者端末上で復号されたコンテンツを無断で複製されたり送信されたりすることを防止できるため、コンテンツの著作権侵害を防止することができる。また、本発明によると、コンテンツに付加する関連情報を誰でも参照でき、当該関連情報の改ざんが防止できるため次のような効果がある。

【００３４】まず、コンテンツに必ず正規の配布対象となった利用者情報を併記することができ、これを誰もが参照できるため、正規の利用者がコンテンツを不正に他者へ流出しないよう注意することになる。また、コンテンツに必ず著作権情報が併記されていて、これを誰もが参照できるようになるため、コンテンツを二次利用したい場合に権利者不明となる恐れがなくなり権利交渉が容易になる。また、本発明によると、コンテンツに必ず、いつ、どこから誰に対して正規に配布されたかの配布情報が併記されているため、誤って海賊版を手に入れてしまったが、同じコンテンツを正規に入手したい場合にコンテンツ入手先を容易に知ることができる。

【００３５】また、本発明によると、以上の効果が汎用＊の表示手段に何ら変更を加えることなく得られる。また、本発明は表示手段を特定していないため、どのようなコンテンツタイプをもつコンテンツにおいても適用可能である。

【００３６】また、本発明によると、図３に示すように、暗号化コンテンツ１と復号ソフト２１と表示手段５を備えていればどの端末でもコンテンツ４が利用可能となるため、例えば、携帯端末２２でのコンテンツ利用が可能になり、正規利用者の私的な複製行為を制限することなく（つまり利便性を妨げることなく）、コンテンツの不正な複製配布が防止可能になる。

【図面の簡単な説明】

【図１】本発明の全体の概要を示す図である。

【図２】従来技術の概要を示す図である。

【図３】本発明の１実施例のシステム図である。

【図４】本発明の１実施例のデータ処理を表すフローチャートである。

【図５】本発明の１実施例のコンテンツの利用方法の概要を示す図である。

【図６】本発明の１実施例のコンテンツの利用方法の詳細を示す第１の図である。

【図７】本発明の１実施例のコンテンツの利用方法の詳細を示す第２の図である。

【図８】本発明の１実施例のコンテンツの利用方法の詳細を示す第３の図である。

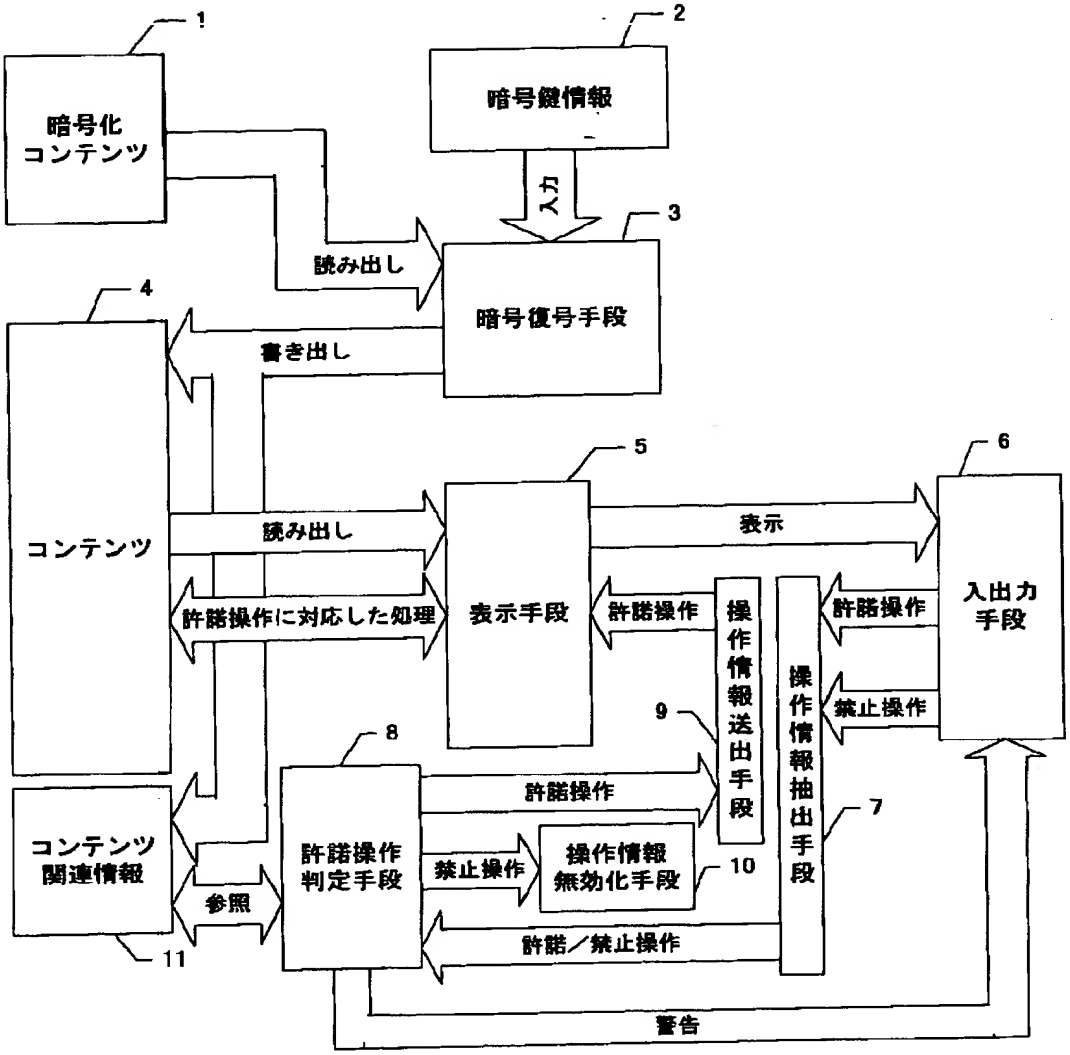
【図９】本発明の１実施例における表示の１例である。

【符号の説明】

１・・・暗号化コンテンツ、２・・・暗号鍵情報、３・・・暗号復号手段、４・・・コンテンツ、５・・・表示手段、６・・・入出力手段、７・・・操作情報抽出手段、８・・・許諾操作判定手段、９・・・操作情報送出手段、１０・・・操作情報無効化手段、１１・・・コンテンツ関連情報、１２・・・コンテンツの二次生成物、１３・・・サーバ、１４・・・コンテンツ紹介情報、１５・・・ブラウザ要求処理部、１６・・・暗号処理部、１７・・・情報発信・アクセス制御部、１８・・・インターネット、１９・・・端末、２０・・・ブラウザ、２１・・・復号ソフト、２２・・・携帯端末、２３・・・揮発性記憶、２４・・・不揮発性記憶、２５・・・複製・編集判定手段、２６・・・フック、２７・・・メッセージキュー、９０１・・・表示手段の画面例、９０２・・・メッセージー操作対応表、９０３・・・表示手段名

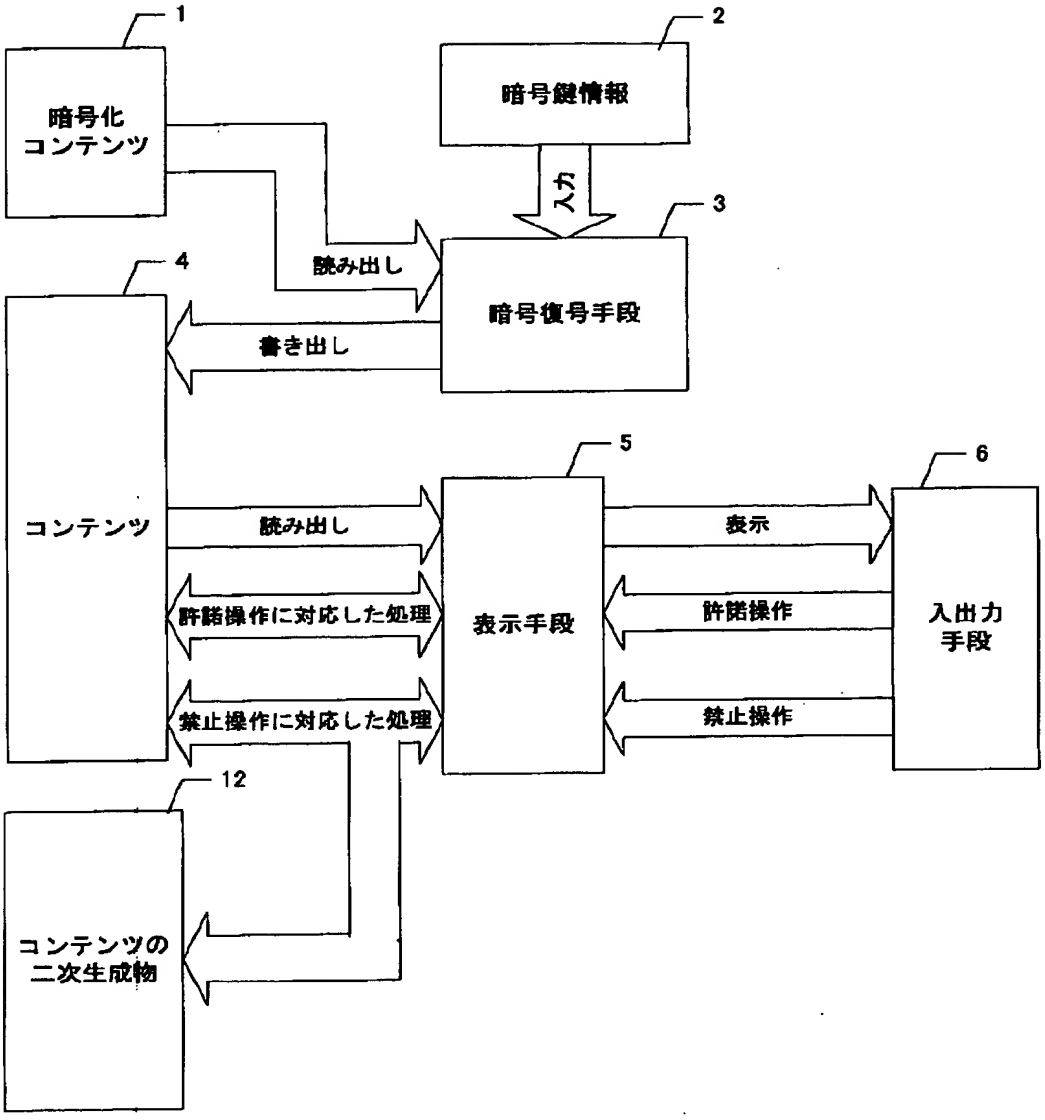
【図１】

図1


1
暗号化
コンテンツ
2
暗号鍵情報
入力
3
読み出し
暗号復号手段
4
書き出し
コンテンツ
5
6
読み出し
表示
許諾操作に対応した処理
表示手段
許諾操作
操作情報送出手段
操作情報抽出手段
許諾操作
入出力手段
禁止操作
9
8
許諾操作
コンテンツ関連情報
許諾操作判定手段
禁止操作
操作情報無効化手段
10
7
参照
許諾／禁止操作
11
警告

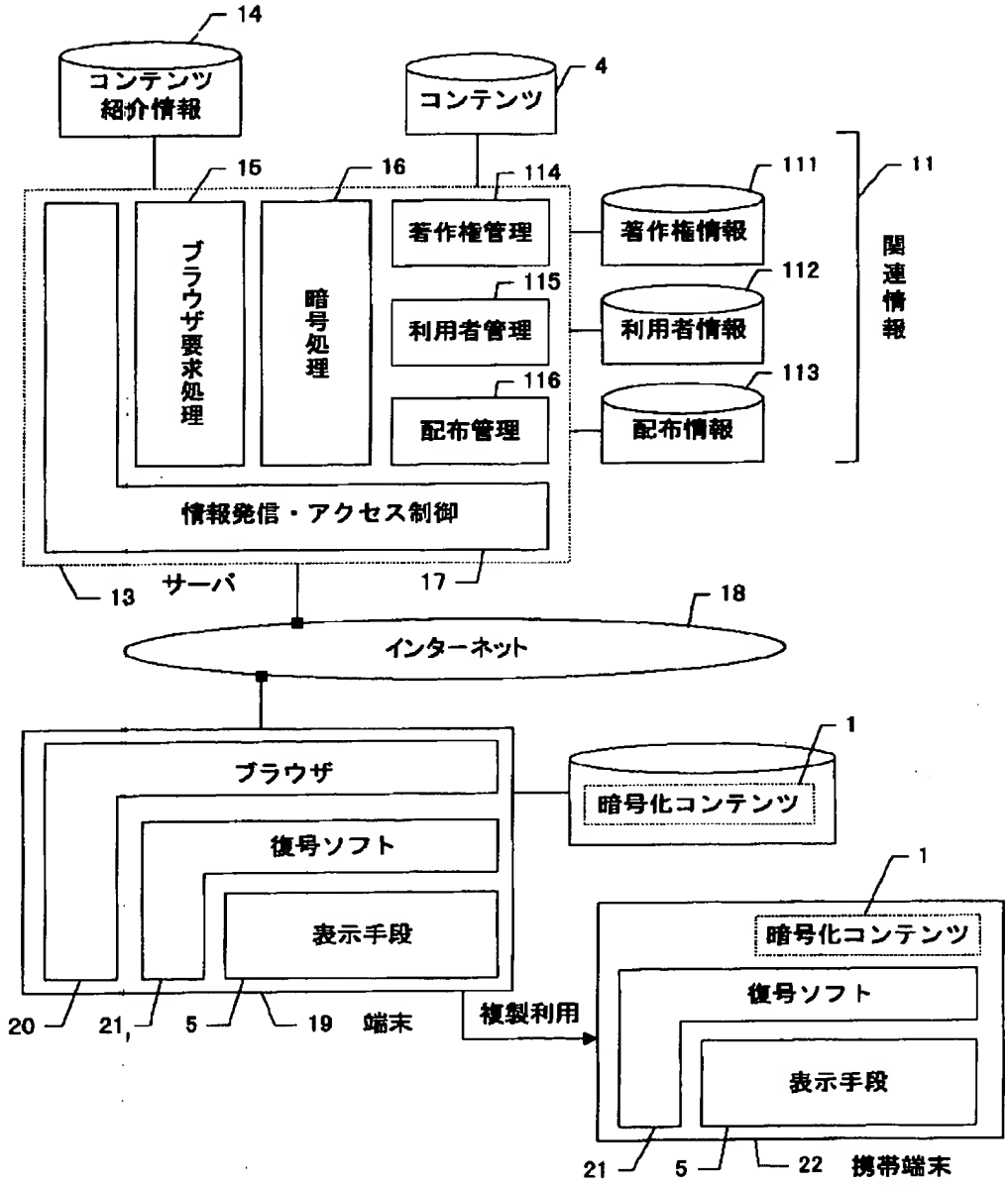
【図２】

# 図2


1
暗号化
コンテンツ
2
暗号鍵情報
入力
3
読み出し
暗号復号手段
4
書き出し
コンテンツ
5
6
読み出し
表示
許諾操作に対応した処理
表示手段
許諾操作
入出力
手段
禁止操作に対応した処理
禁止操作
12
コンテンツの
二次生成物

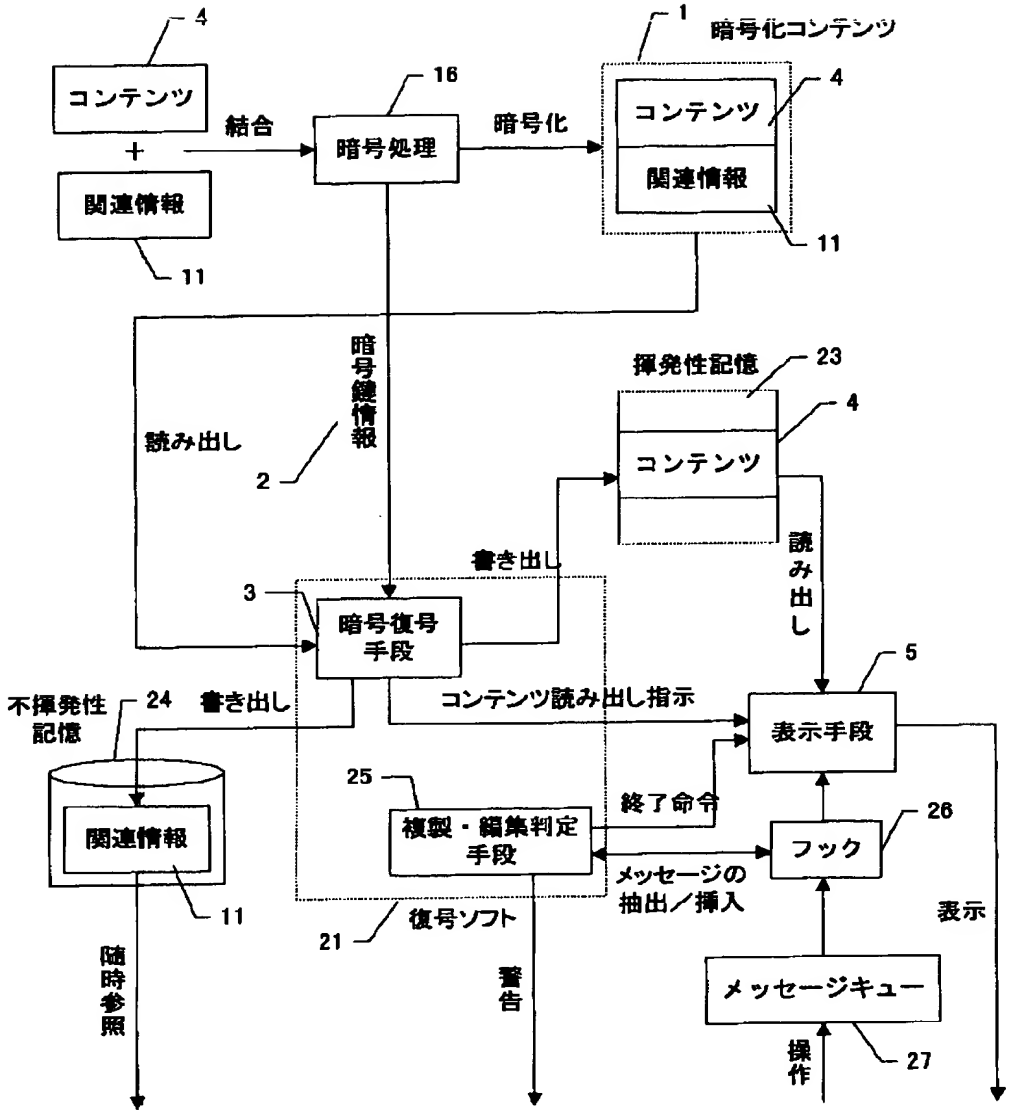
【図３】

# 図3


14
コンテンツ紹介情報
4
コンテンツ
15
16
114
111
11
著作権管理
著作権情報
関連情報
ブラウザ要求処理
暗号処理
115
112
利用者管理
利用者情報
116
113
配布管理
配布情報
情報発信・アクセス制御
13
サーバ
17
18
インターネット
1
ブラウザ
暗号化コンテンツ
復号ソフト
表示手段
1
暗号化コンテンツ
復号ソフト
表示手段
20
21
5
19
端末
複製利用
21
5
22
携帯端末

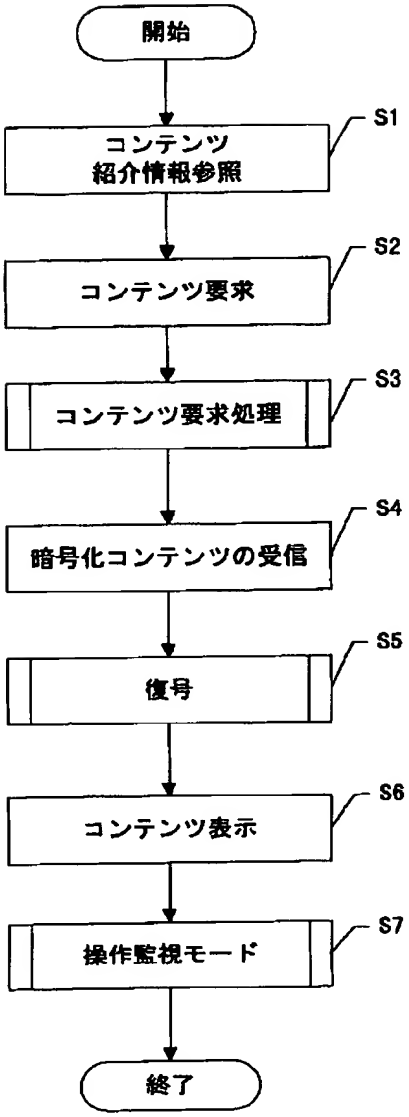
【図４】

# 図4


4
コンテンツ
＋
関連情報
11
結合
16
暗号処理
暗号化
1
暗号化コンテンツ
コンテンツ
関連情報
4
11
暗号鍵情報
2
読み出し
揮発性記憶
23
4
コンテンツ
書き出し
3
暗号復号手段
読み出し
5
不揮発性記憶
24
書き出し
コンテンツ読み出し指示
表示手段
25
関連情報
11
複製・編集判定手段
終了命令
フック
26
メッセージの抽出／挿入
表示
21
復号ソフト
警告
随時参照
メッセージキュー
操作
27

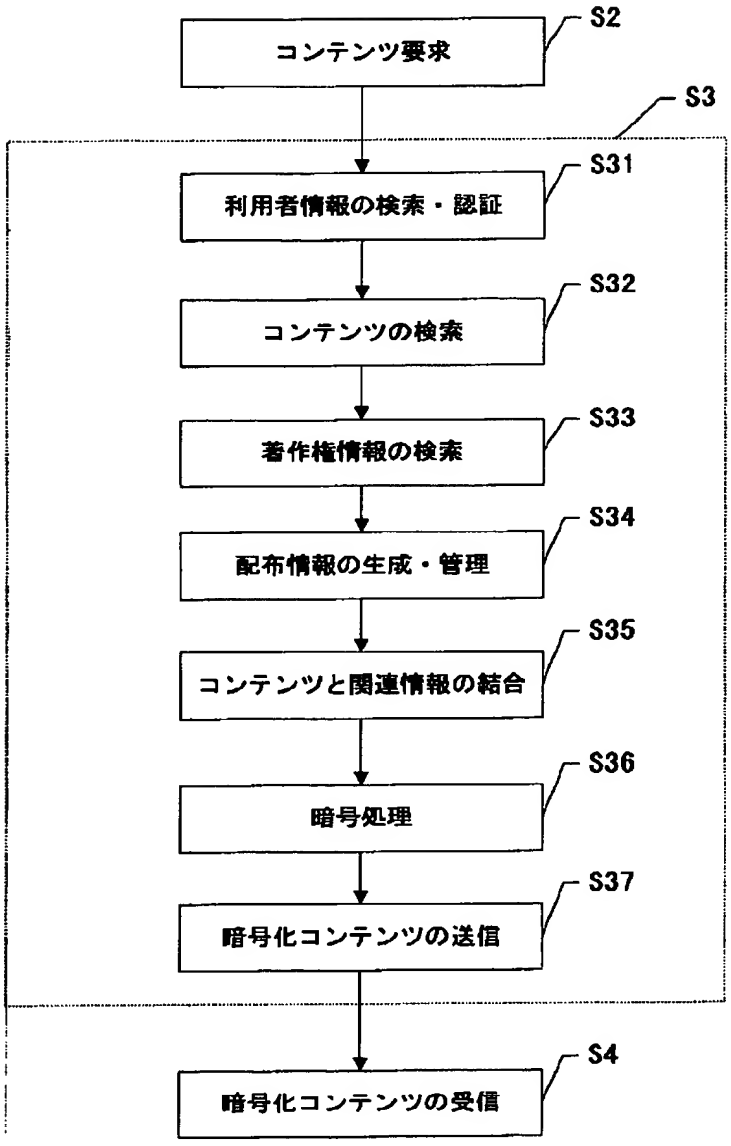
【図５】

図5


開始
コンテンツ
紹介情報参照
S1
コンテンツ要求
S2
コンテンツ要求処理
S3
暗号化コンテンツの受信
S4
復号
S5
コンテンツ表示
S6
操作監視モード
S7
終了

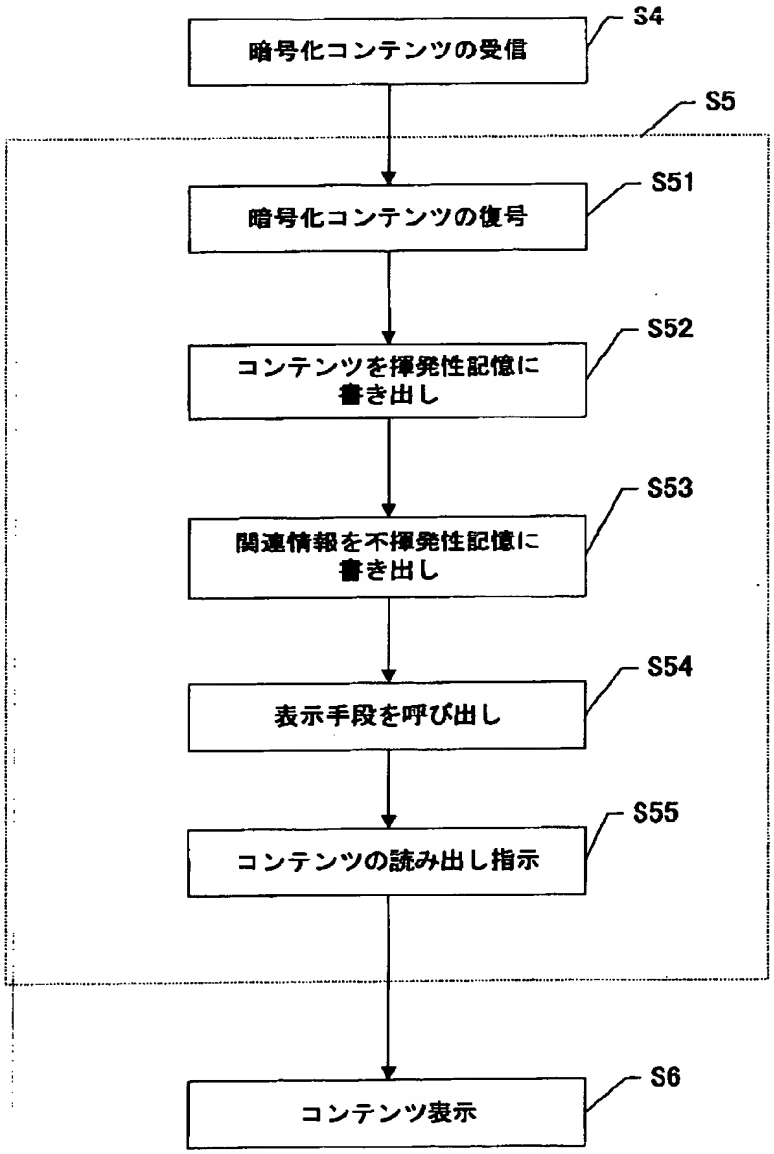
【図６】

図6


コンテンツ要求
S2
S3
利用者情報の検索・認証
S31
コンテンツの検索
S32
著作権情報の検索
S33
配布情報の生成・管理
S34
コンテンツと関連情報の結合
S35
暗号処理
S36
暗号化コンテンツの送信
S37
暗号化コンテンツの受信
S4

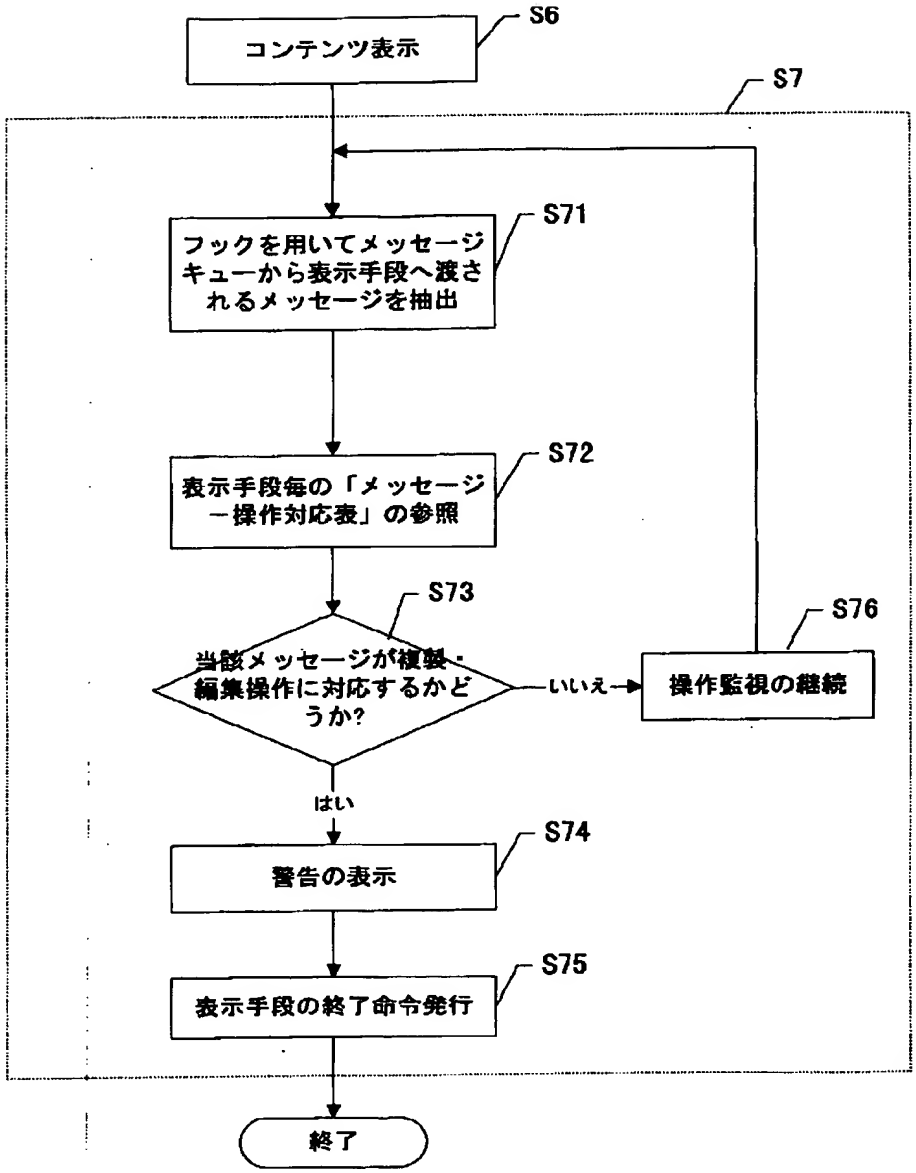
【図７】

# 図7


S4
暗号化コンテンツの受信
S5
S51
暗号化コンテンツの復号
S52
コンテンツを揮発性記憶に書き出し
S53
関連情報を不揮発性記憶に書き出し
S54
表示手段を呼び出し
S55
コンテンツの読み出し指示
S6
コンテンツ表示

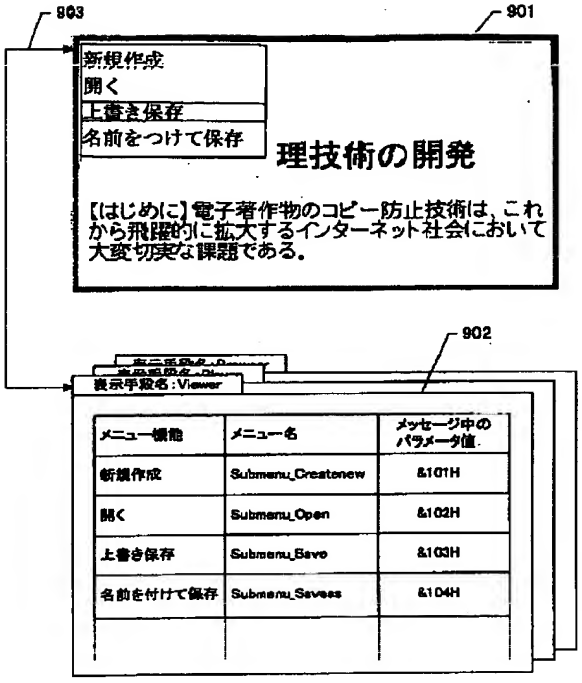
【図８】

# 図8


S6
コンテンツ表示
S7
S71
フックを用いてメッセージキューから表示手段へ渡されるメッセージを抽出
S72
表示手段毎の「メッセージ－操作対応表」の参照
S73
当該メッセージが複製・編集操作に対応するかどうか?
いいえ
S76
操作監視の継続
はい
S74
警告の表示
S75
表示手段の終了命令発行
終了

【図９】

**図9**




---

フロントページの続き

| (51) Int. Cl.[6] | 識別記号 | 庁内整理番号 | FI | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｇ０９Ｃ　1/00 | ６６０ | | Ｇ０６Ｆ　15/20 | ５６４Ｚ | |
| | | | | ５７０Ｍ | |

(72)発明者　水野　勉
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内